

Klassische Sicherheitslücken

Autoren: Sebastian Schreiber, Stefan Arbeiter

Im Bereich der Computersicherheit ist die IT-Branche vor der falschen Wahrnehmung von Problemstellung durch die Öffentlichkeit nicht sicher. IT-Sicherheit scheint es nicht zu geben, denn 14 Jährige Programmierer können scheinbar ohne weiteres ganze Industriekonzerne ohne weiteres lahm legen. Tatsächlich verstecken sich hinter medienwirksamen Hacks oft eine Reihe von bekannten Sicherheitsproblemen, die dann und wann in unterschiedlicher Form auftauchen, was Sicherheitstest auch regelmäßig bestätigen:

1.) Schlechte oder nicht vorhandene Passworte

Ein Angreifer muss keine besonderen Kenntnisse besitzen, um den Firmennamen des Ziels als Passwort auszuprobieren, oder Standard-Paßworte von Massenprodukten (Z.B. die von WLAN fähige SOHO-Routern oder Telefonanlagen) zu recherchieren. Auch Benutzername plus eine laufende Nummer können von Passwortprüfprogrammen wie John1 oder LC (L0phtcrack)2 angeklopft werden. Besonders problematisch ist, dass wenn ein Einbruch möglich ist, weil ein schwaches Passwort verwendet wurde, dieser nur schwer nachvollziehen ist, werden doch die o.g. Passworte zuerst ausprobiert. Hinweise auf vorgehende Versuche fehlen, der Angreifer wurde schliesslich regulär authentifiziert. Werden flächendeckend schwache Passworte verwendet, muss jeder Schutzmechanismus letztlich versagen - dem kann nur ein regelmäßiges Audit vorbeugen, für das z.B. die o.g. Programme verwendet werden können.

2.) Administrative, unnötige und fehlerbehaftete Dienste sind im Internet erreichbar.

Vieles von dem, was oft als "Hacker-Angriff" bezeichnet wird, ist nur das Ausnutzen der Tatsache, das die Dienste eines beliebigen Systems direkt über das Internet erreichbar sind, obwohl sie gar nicht genutzt werden. Durch die "Schwemme" der Würmer, die eine Reihe von Microsoft RPC-Schwächen ausnutzen, wurde zwar bekannt, das es wichtig ist diese Dienste unerreichbar zu machen bzw. patchen, dennoch sind auch immer wieder administrative Dienste, von VNC über Microsoft Terminal-Server bis hin zu telnet und ssh erreichbar. In der Kombination mit 1.) stellen diese ein nicht tragbares Risiko dar, insbesondere wenn Passworte wie bei telnet unverschlüsselt werden. Der erste Schritt, der aber vollständig und ohne Fehler vollzogen werden muss, ist das blockieren aller unnötigen Dienste von Internet-Seite aus mittels eines Paketfilters (Firewall) - mit einem Portscanner wie z.B. nmap 3 gilt das dann das Ergebnis der Arbeiten zu prüfen,

3.) Trügerische Sicherheit durch fehlende Überprüfung

IT-Sicherheit hört leider nicht damit auf, das eine Software über eine Checkbox "Sicher" verfügt, die man anklicken kann - oft genug stellt sich heraus, das der Klick etwas bewirkt, das am Sicherheitszustand nichts ändert, wenn z.B. weitere Dienste ebenfalls erreichbar sind wie unter 2.) oder auf dem Papier "sichere" Konzepte eben nicht sicher umgesetzt wurden - wobei oft auch die Schuld nicht auf der Seite desjenigen zu suchen ist, der dies vorgenommen hat:

Allein Bezeichnungen innerhalb von Software können zu fatalen Fehlentscheidungen bei der Konfiguration führen: So bieten kleine SOHO-Router manchmal eine "DMZ"-Einstellung an, um für eine interne IP-Adresse alle Ports freizuschalten - ohne aber über einen separaten Anschluss für dieses System zu verfügen. Normalweiser ist die DMZ, die Zone in der sich die Systeme befinden die vom Internet aus erreichbar sein müssen, auch physikalisch vom Rest des Netzes getrennt

Das Anklicken der Übertragungsart "Sicher" bei Web-Seiten, die anschliessend HTTPS anbieten gehört ebenfalls in diese Kategorie: Der drauffolgende Prozess der Zertifikatannahme ist für viele Anwender nicht transparent: Wer würde sich z.B. an einem roten Kreis bei einem Zertifikat stören, der auf SSL-Spoofing hindeuten könnte?

Typisches Beispiel wäre auch SSH, die Secure Shell, die "sicherer ist" als telnet - dennoch aber in der Vergangenheit ebenfalls Sicherheitslücken besass, als gepatcht und gepflegt werden muss, wie jede andere Software auch. Schliesslich bietet SSH die Sicherheit durch den verschlüsselten Transport der Daten und der Authentifizierung, nicht generell durch die blosse Anwesenheit - die Bezeichnung "crypted shell" wäre vielleicht besser gewesen.

Sicherheitsrisiken, die durch die Punkte 1-3 bestehen, sind seit langem bekannt, dennoch scheinen sie nicht zu verschwinden. Mit der kommerziellen Ausnutzung durch Spammer und DDOS Erpresser bedeutet das Betreiben unsicherer Systeme aber auch, anderen ebenfalls ein Risiko zuzumuten: SPAM von einem kompromittierten System im eher harmlosen oder ein DOS-Angriff im eher schweren Fall. Inwieweit über neue Sicherheitskonzepte geredet werden muss, wenn die Schlagkraft der alten sich noch nicht voll entfalten konnte, ist daher fragwürdig.